The Elite Hackers of the FSB

By BR Data

Archived: 2026-04-06 03:11:13 UTC

For almost two decades, hackers with Snake have been forcing their way into government networks. They are considered one of the most dangerous hacker groups in the world. Who they work for, though, has always been a matter of pure speculation. But reporters with the German public broadcasters

and

have discovered some clues, and they all lead to the Russian secret service FSB.

Die deutsche Version dieses Artikels finden Sie hier.

“One of the longest running and technically proficient threat groups in operation.”

“They target foreign governments. With intelligence service methods. To provide their own government with an informational advantage.”

“It is the Holy Grail of cyberespionage.”

Chapter 1 - #notagame

Whenever employees of the Federal Office for the Protection of the Constitution (BfV), Germany’s domestic intelligence agency, sit down for a game of quartets, they are happy to get their hands on the H2 card. It is one of the most powerful cards in the game, one which promises a quick victory. After all, it represents one of the best hacker groups in existence. The card is printed with a reddish-brown cobra that is winding itself around a server rack and crushing it. In the upper left corner of the card is the name of the hacker group: Snake.

A participant in the BfV’s apprenticeship program developed the quartets game, and since then, it has been a gift item the agency presents to diplomats and members of other secret services and agencies. Even if the hashtag associated with the game is #notagame, that is actually precisely the point of the deck of cards: They are a playful way to learn about the hacker groups in existence and how dangerous they are.

There are five categories in the card game: pain factor, capabilities, defensive ability, sophistication and danger index.

The Snake hackers are also known by the names Turla or Uroburos.

The group is thought to have been active at least since 2004.

Snake is one of three groups in the card game thought to be the most dangerous, with 10 out of 10 points on the danger index.

It is rather striking that the quartets cards provide no information regarding who the 32 hacker groups included actually work for. The card on which the rules of the game are printed merely reads: “Due to the significant resources available to the attackers, it is assumed that a majority of the APT groups are controlled by secret

services.” APT stands for “advanced persistent threat,” an appellation applied to hacker groups that have sufficient time and expertise to covertly penetrate IT networks – essentially master thieves who are rarely caught. State-sponsored espionage that follows fiber-optic cables into server racks and squeezes out their secrets bit by bit, just as portrayed in the image on the Snake card. Snake’s targets include defense contractors, nuclear research agencies and foreign and defense ministries.

IT security companies and government agencies in Germany and around the world have been monitoring the Snake hackers for several years. The investigators do not, of course, print their findings on quartets cards. Rather, they pack them into reports for the Chancellery in Berlin, or for the Federal Public Prosecutor General’s office in Karlsruhe. The investigators are charged with finding out who the hackers are working for, and with turning up evidence strong enough to convince a judge to issue an arrest warrant.

The Snake hackers, after all, have also been active in Germany. They were able to penetrate the network of the German Foreign Ministry and are thought to have had free rein for a full year before they were discovered in late 2017. A criminal investigation has been underway since then, although queries about that investigation went unanswered.

According to IT security experts, learning who hackers work for is difficult. Digital tracks can easily be covered, and falsifying documents is also rather simple. When evidence is uncovered – for example when investigators are monitoring a server and are thus able to watch hackers as they work – it is usually classified as confidential. The public tends to learn nothing about it. Otherwise, the hackers would figure out they were under observation and change their tactics.

It is precisely this secrecy, however, that is so convenient for many countries. On the one hand, they are able to continue their spying and access important information. On the other, though, they can simply deny being involved in cyberespionage when they are publicly accused of such acts.

In the case of Snake, for example, Britain’s National Cyber Security Centre (NCSC) writes that the hackers are “suspected to be Russia-based.”

The Estonian secret service is more direct and claims that the hackers work for the Russian domestic intelligence agency FSB. Neither the British nor the Estonians, however, provide any evidence for their claims.

But there are many clues indicating that the hackers with Snake have worked for the FSB, as this investigative report from BR and WDR will show. The investigation began with a tipoff from an IT security expert that was rather vague, not much more than a single sentence. The hackers, the IT expert wrote, had made critical mistakes, though several years had passed since then. Thanks to this tip, however, a team of reporters was able to find and follow a series of digital tracks. And almost all of them were freely accessible on the internet, and not hidden away in classified intelligence reports. They are clues that may seem meaningless at first glance, but when they are all put together, they lead directly to the front door of one of the most powerful secret services in Russia: The FSB.

This is the first time that these tracks have been publicly documented, the product of months of reporting revealing just how long cyberespionage has apparently been a commonly used tool of Russian intelligence services. The reporting stretches almost 20 years into the past, leading to people who likely developed the malware used by Snake. One of the suspected developers brags on his website that he once worked for the FSB.

Additional clues can be found in Russian- and English-language forums and on sites like LinkedIn and Facebook. Ultimately, the reporting leads to a company in the Russian city of Ryazan – a company that, according to official information, once belonged to the FSB.

Chapter 2 – The Tools of the "Geniuses"

For this article, reporters from BR and WDR spoke with more than 20 experts and examined internal reports from two respected IT security companies. The reports confirm information the reporters gathered on their own.

Many of the experts asked that their names not be published. Some are not allowed to speak with the press, while others say they would prefer to avoid getting "beat up" by FSB agents. The Russian intelligence agency is extremely unpredictable, and FSB agents are thought to be responsible for the poisoning of Russian opposition politician Alexei Navalny, among other transgressions. Russia has denied any involvement in the poisoning and no investigation has been initiated. Instead, the authorities arrested Navalny and he is currently imprisoned in Russia.

"Yet I would love to buy a beer for these guys," said one expert who has analyzed the hacking operations performed by Snake. Without any preparation, he spoke on the phone for more than an hour about malware that he last examined several years earlier. When asked how he could remember even the smallest details so well after such a long time, he said: "Understanding and stopping their attacks was among the highlights of my professional career."

The level of proficiency of the Snake hackers is outlined in documents that were leaked several years ago. The Canadian signals intelligence agency, which calls the group Makers Mark, described the developers of the malware at the time as "geniuses," but said their highly complex tools are "implemented by morons." An official from a German security agency explains it as follows: "For some tasks, such as programming the malware code, people who are extremely technically adept are required. But those who then gather up the goods once a network is penetrated – they don't have to be the best."

BfV, the German domestic intelligence agency, also emphasizes the "exceptional" abilities of the hackers, who present an "extreme danger" (PDF).

IT security researcher Paul Rascagnères, who in 2014 became one of the first to discuss Snake in public, told BR and WDR: "For me, at the time, they were perhaps in the top five worldwide." Many hacker groups, he says, learned how to successfully penetrate networks by watching Snake.

The trick that Snake used in Germany also serves to demonstrate just how clever the hackers can be. They chose a rather unusual path to their target: via outer space.

It was Tuesday, Dec. 19, 2017, when German security officials received the tipoff. A foreign intelligence service informed the Bundesnachrichtendienst (BND), Germany's foreign intelligence service, that somebody had hacked into the IT system belonging to Germany's Foreign Ministry.

The Federal Office for Information Security (BSI) in Bonn immediately sent experts to Berlin. A mobile incident response team spent several weeks scouring the Foreign Ministry network to find the hackers.

The attack by Snake, according to a description provided by a BSI employee during a non-public session of German parliament, was “professional and extremely delicate and pursued with great patience.” Great patience was essentially a reference to the fact that the hackers spent almost a year in the network before being detected.

BSI agents learned that the hackers found their way into the Foreign Ministry via a detour through the University of the Federal Public Administration. The institution provides training to security officials, police and diplomats in addition to intelligence agents, both foreign and domestic.

Together with the Foreign Ministry, the BSI decided to adopt a strategy that, at first glance, might appear to be extremely risky. Instead of shutting the hackers out of the network, they decided to monitor their activities for several weeks.

The analysis performed by the BSI revealed the trick with the satellites. Whereas fiber-optic cables are the primary method used in Germany for accessing the internet, other countries rely heavily on satellite internet. The data is simply sent from space directly to the user’s satellite dish. The Snake hackers are able to take advantage of that delivery method.

The malware from Snake infects the computers of the Foreign Ministry. The malware includes a link to a specific website.

The infected computer seeks to access the website, which is controlled by the hackers. In doing so, the computer is forced to use satellite internet.

The Foreign Ministry computer sends the data into space, and a satellite then sends it back down to earth.

The Snake hackers are then able to collect the data using their satellite dishes.

Satellites spread data across an extremely broad area, sometimes even across an entire continent. That means that nobody knows exactly where the servers belonging to Snake are located. But without confiscating the servers, it is difficult to completely block an attack.

In late February 2018, the BSI decided it had seen enough. And the hackers hadn’t actually stolen all that much by the beginning of 2018 – a total of six documents, only one of which was classified. Nevertheless, the BSI decided to throw the hackers out of the network. A short time later, public prosecutors launched an official investigation into the cyberintrusion.

Germany’s Federal Office of Criminal Investigation (BKA) branch in Meckenheim was tasked with leading the investigation. Located in the small town just outside of Bonn, the branch is home to the BKA division responsible for espionage cases. It is one of several cyberespionage cases that are thought to have had their origins in Russia.

But who do the hackers with Snake work for?

Chapter 3 – vlad

One of the first clues on the trail that ultimately led the team of reporters to the creators of Snake was a pair of usernames. The hackers had forgotten to delete them from the computers on which they developed the malware. “They probably left them in there by mistake,” Adrian Nish, of the British IT security firm BAE Systems, told BR

and WDR. Snake develops malware in teams, and to ensure that nothing gets lost, they use a program that tracks which team member contributes what line of code. “They should have removed that information,” Nish says.

The names, which could now be read by everybody, were: vlad and urik.

But how helpful could these names actually be for further investigations? Vlad could stand for at least three different male first names: Vlad, Vladislav or Vladimir. Urik likely stands for Yuri. Those names, though, are hardly rare in Russia. You might as well be in a city like Detroit looking for someone named Mark, Mike or Chris. On their own, the names were practically meaningless.

But Snake, as indicated on the H2 card of the BfV’s quartets game, has been in operation since 2004. And that’s an important snippet of information because both the internet and the operating systems then in use were different than they are today. Companies like Microsoft did not provide documentation back then for much of their software, meaning that computer experts turned to forums and listservs to exchange information on how the operating systems actually worked. These discussions are still on the internet, freely accessible to all. In one forum, several Vlads are involved in the exchanges, but one of them is particularly striking. In this article, we will refer to him as Vlad from the forum.

In the early 2000s, he posted a software program. Vlad from the forum referred to it as a first attempt one which he considered to be provisional.

Put simply, the program was a kind of filter, as IT experts describe it. It would analyze inbound connections to the network and check them to determine if they adhered to a certain pattern. Two years after Vlad from the forum posted his code on the internet, the Snake hackers used a similar filter in their malware. By way of the filter, the hackers were able, for example, to determine what documents were stored on the computer they were currently scrutinizing.

Two Vlads and two filters that work in pretty much the same ways. Striking to be sure, but is that sufficient to prove a connection? Countering that idea is the fact that the code used by Snake is far more complex than the version that is freely available on the internet, as an IT expert, who asked to remain unnamed, explains. “We stumbled across this forum and Vlad in 2014,” he says. He and others discussed what they had found, he says, but didn’t draw any firm conclusions.

A second IT security expert says that he also crossed paths with Vlad from the forum in 2014 but didn’t pursue the lead. Sure, he allows, there are similarities, but it is also possible that someone just copied the code and developed it further. After all, it was open to all, and anyone looking for a network filter would have necessarily happened upon this code. “In any case, I certainly wouldn’t bet my house that it’s the same person,” he says today.

But it is precisely this clue that leads directly to the FSB.

Vlad from the forum revealed his full name and email address, as can be seen from the forum entries. But his full name is likewise extremely common. Essentially, instead of looking for someone named Mike, the search was now for a Mike Smith.

In 2007, the Russian Education Ministry began seeking participants for a course on programming firewalls. The instructor had the same name as Vlad from the forum – who had also made a firewall available for download.

According to information posted by Vlad himself, he lived in Ryazan, around 200 kilometers from Moscow. The course description included an email address that Vlad had used to publish both personal projects as well as scientific articles.

An article from 2011 noted that Vlad was a student at the Ryazan State Radio Engineering University and his studies were focused on recognizing “network attacks.” Vlad published the article together with the head of the department for information security. This department head was both extremely well connected with the FSB in Ryazan and a member of a council of Russian universities, which has close ties to the FSB Academy.

Vlad from the forum, as the reporters learned, certainly possesses the same expertise as the vlad who forgot to delete his name from the Snake malware program. Both are specialized in firewalls.

An additional, technical clue enters the picture here, one which seems to show that the two Vlads are actually the same person. The clue was discovered by the IT security companies Crowdstrike and BAE Systems. Crowdstrike maintains a database of malware that contains billions of files. The company was able to determine that the two Vlads used the same folder structure on their computers. This information was included in the data itself – both in the firewall project belonging to Vlad from the forum and also in the malware program produced by vlad. In an internal report from August 2021, which the reporters were able to review, the company writes that it had been looking for precisely this folder structure, noting that it was only used by these two Vlads. That would indicate, the report notes, that the datasets were “developed by the same person.” Which means there is apparently just one Vlad. First, he posted the firewall project to the web and later began programming malware for Snake.

Scientific articles written by Vlad note that he worked in 2011 as a department head for a company in Ryazan called Center-Inform. For a time, from 2004 to 2007, the company Center-Inform was officially a part of the FSB, Russia’s domestic intelligence agency.

Chapter 4 – “Atlas of the FSB”

The company’s headquarters are located in St. Petersburg, and it has a total of 17 branches in different Russian cities, from Moscow to Vladivostok. Center-Inform has received state licenses from a number of public agencies, among them the FSB, which licenses the company to protect sensitive data and process state secrets. The branch office in Ryazan – the city in which Vlad was employed by the company – was explicitly authorized to access such secrets.

Center-Inform’s company history is laid out on its website, according to which the company developed within an intelligence service called FAPSI, which specialized in monitoring radio and internet surveillance. When this agency was dissolved in 2003 by Russian President Vladimir Putin, the department for “information acquisition” was transferred to the FSB. That apparently also included Center-Inform.

Center-Inform was integrated into a company, the name of which would include FSB for a few years. It was called Atlas. Atlas developed mobile phones that were allegedly immune to monitoring, referred to as “bumblebees” in the Russian media.

The company’s client list includes almost all high-ranking positions within the Russian administration:

The presidential office

The Interior and Foreign Ministries

Three intelligence agencies, including the FSB

Between 2004 and 2007, the company was officially referred to as “Atlas of the FSB.” This connection can also be seen in official press releases posted to the FSB website. Atlas is described there as a developer of the “newest technologies.”

Just how closely connected Center-Inform, Atlas and FSB were at the time isn’t just clear from the company histories. Their street addresses – in Ryazan – make it obvious as well.

Two buildings located on Lenin Street – numbers 46 and 48 – stood out during the reporting for this story. The two addresses appear both in online databases and in official documents from the 2000s. Images of the buildings as seen on online mapping services show a joint driveway connecting the two buildings.

The Russian business register makes it clear that number 48 is home to a division of FSO, a service with espionage capabilities widely referred to as Spezsvyaz and which is tasked with securing the communications of the Russian government and the president. Next door, in building number 46, was the local FSB branch. Atlas, for its part, was listed under both addresses.

The telephone number that Vlad used for his 2007 firewall course is also listed in registration databases for websites. It is listed as the official number for the Atlas branch located on Lenin Street 48.

Chapter 5: Urik

The second username from the Snake malware program, Urik, is also extremely common. In Russian, it is frequently used for a friend that you’ve known for a long time. It is a nickname for Yuri.

Ryazan in the 2000s was home to a small, technically adept community that offered web-hosting services and issued email addresses. The role that this community played is apparently of such great interest today that the German BND intelligence agency held a workshop on it, according to information collected by BR and WDR. Vlad had an email address from the community, as did the Center-Inform branch, which belonged to the FSB at the time. And a certain Urik also had an e-mail-address from the community.

Urik was a frequent participant in Russian-language forums for people who enjoyed working on their cars. In his profile, Urik’s place of residence is listed as Ryazan, where Vlad also lives. A search of social networks reveals that he also attended the same technical university. And he claims openly to be an expert in computer espionage.

Urik has profiles on a variety of social networks, in which he provides a comprehensive look at his career. On his website, he writes that he worked for FSB for 10 years, with the precise years listed in social networks: from 2003 to 2013. His customers, he claims, consider him to be the best information security expert in the Russian-language internet. He holds lectures at conferences about how to defend against attacks on websites and claims to have built up the server infrastructure for large companies. In an interview that can be found on YouTube, he says of his work for FSB that he focused on “computer espionage and counterespionage.” In another presentation, unearthed by Crowdstrike, it reads that Urik also worked for Center-Inform – and was responsible for “foreign computer espionage”, on behalf of the FSB. His Facebook profile was no longer online at the end of 2021.

At this point in the reporting, events begin repeating themselves. Regarding Urik, in any case, there isn't any more that can be said without revealing his identity. And with other usernames that the hackers left behind in the malware source code, the trail also seems to lead back to Ryazan.

One of those names, for example, is gilg. A user by the same name opened a discussion on a Russian-language forum in 2006 that apparently led a few years later to the U.S. completely reconsidering its cybersecurity strategy. A couple of USB sticks led to the move.

These days, it is common knowledge that sticking unknown USB sticks into your computer can be dangerous. Who knows, after all, what might be on the thumb drive. Snake is one of the reasons why the world has become so careful.

In 2008, the hackers distributed a number of USB sticks, allegedly at parking lots belonging to a U.S. military base in the Middle East. One soldier apparently picked up one of the USB sticks and plugged it into his computer. A malware program installed itself on the computer via the stick, essentially providing the hackers with a gateway into the military's network – a network normally not connected to the internet that was used to coordinate the military operations in Afghanistan and Iraq. When the cyberintrusion was discovered in October 2008, it was referred to as the "most significant breach of U.S. military computers ever." Plugging USB sticks into computers was immediately prohibited.

A user by the name of gilg, in this forum, discussed a technique which was extremely consistent with the details of this intrusion. The IT security company BAE Systems lists four such discussions that suggest gilg was talking about technologies that would subsequently be used by Snake for cyberespionage.

Ultimately, it is a number of tiny details that only form a complete picture once they are assembled.

And that picture indicates that vlad and urik are likely two of the developers behind the notorious malware program used by Snake. An analysis of the various versions of the malware program suggests that the two consistently modified, expanded and improved the software over the course of several years. The geniuses referred to by the Canadian intelligence service in its presentation likely included these two.

Today, it seems that vlad and urik no longer work for Snake. For that reason, BR and WDR decided not to publish the full names of the developers. The illustrations used here are based on real images, but they have been altered. But their tools were still in use in 2020.

Neither the suspected developers of the Snake spy software nor the companies Atlas and Center-Inform responded to our efforts to contact them. The FSB also declined to answer questions from BR and WDR.

The Russian Embassy responded by saying it has "become a trend" to speculate about "Russian hackers." The statement continues: "We believe it is inappropriate to comment on speculation and fakes in the mass media." German officials, the embassy continued, have been "requested to cease with the megaphone-diplomacy and keep the discussion of questions pertaining to cybersecurity to the experts." The embassy referred to a meeting on the issue that took place on Sept. 2, 2021, in Berlin within the auspices of the German-Russian High Level Working Group on Security. Fighting cybercrime, the embassy said, is a global problem that must be addressed jointly.

The Snake hackers are apparently still active. Recently, the IT security company Cisco wrote that Snake was apparently able to penetrate the government of Afghanistan – in the months prior to the Taliban takeover.

“The Elite Hackers of the FSB” is a joint research of the Bayerischer Rundfunk (BR) with the Westdeutscher Rundfunk (WDR).

Published at 17.02.2022

Authors: Hakan Tanriverdi (BR), Florian Flade und Lea Frey (WDR)
Digital Design: Sebastian Bayerl, Steffen Kühne, Max Brandl (BR)
Editing: Robert Schöffel und Verena Nierle (BR), Monika Wagener (WDR)
